УДК 004.056.5

И.И. Борисенко, Одесса, Украина

ГРАФОВАЯ МОДЕЛЬ ПРЕДСТАВЛЕНИЯ СТЕГАНОКОНТЕЙНЕРА И АНАЛИЗ СОСТОЯНИЯ ЕГО ЗАЩИЩЕННОСТИ

Представлена математическая модель стеганоконтейнера (СК), которая дает возможность оценить его устойчивость к предполагаемой атаке. В качестве инструмента для анализа реакции СК на атаку в графовой модели используется спектр матрицы смежности графа «СК - противник». Разработан метод, позволяющий выполнить анализ возмущений, возникающих при внедрении сообщений различными стеганографическими алгоритмами, что дает возможность сравнивать их эффективность. Приведены результаты вычислительного эксперимента, подтверждающие эффективность предложенного метода.
Ключові слова: *математическая модель стеганоконтейнера, анализ возмущений*

Представлено математичну модель стеганоконтейнера (СК), яка дає можливість оцінити його стійкість до ймовірного нападу. В якості інструмента для аналізу реакції СК на напад в графовій моделі використовується спектр матриці суміжності графа «СК - супротивник». Розроблено метод, який дозволяє виконати аналіз збурень, які виникають під час вбудовування повідомлень різними стеганографічними алгоритмами, що дає можливість порівнювати їх ефективність. Наведено результати обчислювального експерименту, які підтверджують ефективність запропонованого методу.
Ключевые слова: *математична модель стеганоконтейнера, аналіз збурень*

The mathematical model of stego - image (SI) are presented to estimate it noise stability to assumption attack. In the graph model is used the spectrum of adjacency matrix of graph "SI - adversary" for analysis the reaction SI on an attack. The metod allowing to make the analysis of the perturbations, arising in case of embedding of messages different steganografic algorithms, that gives the opportunity to compare their efficiency is constructed. The results of numerical experiment confirm the efficiency of the proposed method.
Keywords: *mathematical model of stego - image, analysis of the perturbations*

Введение

В настоящее время в рамках вычислительных сетей проводится активный оперативный обмен различной медийной информацией в виде звука, изображений, видео между участниками сетевых сеансов независимо от их территориального размещения, поэтому такие информационные потоки широко используются в качестве *контейнеров* для пересылки *секретной информации* (СИ) в открытой информационной среде. Контейнер со встроенной секретной информацией (в дальнейшем *стеганоконтейнер*) при пересылке или хранении может подвергнуться атакам непреднамеренным (шумы в канале связи) или преднамеренным (атаки конкурентов, заинтересованных лиц). В любом случае в дальнейшем объекты, субъекты,

события, ставшие причиной нарушения целостности стеганоконтейнера (СК), будем называть – *противник*. Понятно, что чем больше атакующее воздействие, тем большая степень разрушения СК вплоть до его уничтожения. Будем считать, что, атакуя СК, противник не намерен себя обнаружить, т.е. атакующее воздействие должно быть таким, при котором обеспечивается надежность восприятия – атака зрительно не заметна.

Универсальных систем и средств защиты информации (СЗИ) на все случаи не существует, т.к. каждая защита создается для конкретной информационной системы, ее окружения и внешней среды, под конкретные угрозы, функциональные требования и требования гарантии защиты [1]. При их изменении система защиты должна быть способной адаптироваться к ним. В связи с этим очень важным становиться вопрос, к каким атакам СК будет устойчивым, а к каким нет.

Цель статьи и постановка задач

Целью данной работы является разработка графовой модели СК, дающая возможность за счет учета различий в результатах воздействия атаки на СК, сформированного различными стегоалгоритмами, выбрать наиболее устойчивый из них в зависимости от предполагаемой возможной атаки.

Для достижения поставленной цели необходимо решить следующие *задачи*:

1) определить структурные элементы СК для построения его графовой модели;

2) построить граф противника и формализовать атакующее воздействие на СК;

3) разработать метод оценки устойчивости СК предполагаемой атаке;

4) провести вычислительный эксперимент.

Основная часть

Каким бы образом не выполнялось стеганопреобразоване (СП) – пространственной области, частотной или спектра матрицы контейнера, оно неминуемо приведет к изменению значений некоторых (всех) его элементов, что свидетельствует о том, что они являются носителями встроенной информации. Такие элементы будем называть *информационными элементами* (ИЭ). Любая атака, действующая на СК, по-разному отразится на ИЭ: в некоторых из них информация будет разрушена полностью, а для других ИЭ атака окажется безопасной. Атаку будем рассматривать как малые возмущающие воздействия, которые не приводят к нарушению требования надежности восприятия СК. Учет различий в результатах воздействия атаки на ИЭ является важным при разработке стегоалгоритмов (СА), а также при установлении устойчивости СК к предполагаемой атаке.

1. Построение графово - матричной модели СК

Будем использовать в качестве модели СК взвешенный граф [2] со структурным отношением «состоять из». Такой принцип был использован для построения графово-матричной модели защищенной информационно-технологической системы [3].

Перейдем непосредственно к построению взвешенного графа-модели СК, представляющего собой дерево.

Шаг1. Определение структурных элементов СК. СК, как информационная система, в целом представляется изолированной вершиной (Рис. 1), не имеющий связи с вершинами подграфа контейнера, который выполняет функции СЗИ: доступа контейнера к информации, циркулирующей в системе нет. Контейнер представляется в виде неперекрывающихся блоков (областей) определенного размера (не обязательно одинаковых), каждому из которых соответствует вершина графа, лежащая во втором уровне корневой структуры. Вершины третьего уровня соответствуют подмножествам элементов контейнера, на которые разбит каждый блок (к примеру блок разбит на восемь подмножеств, обозначенных П1, …, П8).

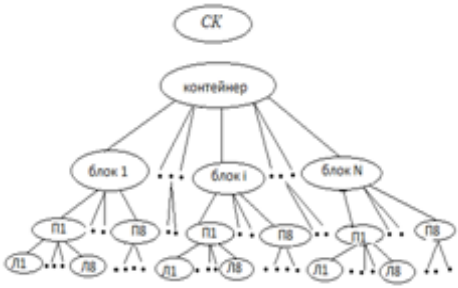

Рисунок 1 – Первоначальный вид графа СК

Каждый последующий уровень представляет собой следующий уровень детализации и определяется выбранным СП. Последний уровень корневой структуры графа представлен элементами контейнера (листья графа), через которые происходит связь с внешней средой и все возможные атаки на СК.

Значения весовых коэффициентов (ВК) листьев взвешенного графа определяются конкретным СА и должны отражать реальную защищенность ИЭ. Вес вершины на каждом уровне корневой структуры графа, кроме последнего (листья), определяется как положительное число, большее или равное сумме весов смежных с ней вершин, находящихся на следующем по порядку уровне корневой структуры.

Шаг 2. Построение матрицы смежности $Madj$ взвешенного графа. Поскольку граф неориентированный, его матрица смежности является симметричной. $Madj$ подвергается нормальному спектральному разложению, в результате однозначно определяются ее собственные значения (СЗ) и собственные вектора (СВ) [4].

Шаг 3. Введение в построенном графе связи СК-контейнер. В результате СЗИ – контейнер получает доступ непосредственно к СИ. Это приводит к тому, что $Madj$ получает возмущение (в результате получается матрица $\overline{Madj}$), а следовательно возмутятся и ее СЗ и СВ. *Совокупность возмущений СЗ и СВ является математическим представлением информации, подлежащей защите, которая находится в СК.*

2. Метод оценки устойчивости СК предполагаемой атаке

Поскольку матрица $\overline{Madj}$ симметрична, то ее спектр содержит хорошо обусловленные вещественные СЗ. Хорошая обусловленность СЗ приводит к нечувствительности всего спектра матрицы $\overline{Madj}$ к возмущающим воздействиям. Иначе говоря, возмущения СЗ по абсолютной величине сравнимы с самим возмущающим воздействием, чего нельзя в общем случае сказать о СВ [3]. Таким образом, об устойчивости СК к предполагаемой атаке, о величине возмущающего воздействия (серьезности атаки), будем судить по величине возмущений СЗ матрицы $\overline{Madj}$. Для количественной оценки величины возмущений СЗ будем использовать относительную погрешность: $\delta = \frac{СЗ_и - СЗ_a}{СЗ_a}$, где $СЗ_и$ – СЗ до атаки, $СЗ_a$ – СЗ после атаки. Заметим, что, как показывает проведенный вычислительный эксперимент, наибольшую относительную погрешность имеют наименьшие по модулю СЗ, относительная погрешность монотонно уменьшается с увеличением модуля СЗ.

Шаг 1. Построение графово - матричной модели противника с матрицей смежности $ATAK$.

Шаг 2. Построение совокупной графово - матричной модели СК и противника. Матрица смежности C совокупной графово - матричной модели является блочно-диагональной: $C = \begin{pmatrix} \overline{Madj} & 0 \\ 0 & ATAK \end{pmatrix}$.

Пока противник не оказывает атакующее воздействие на СК, связи между блоками $\overline{Madj}$ и $ATAK$ отсутствуют (наличие нулевых блоков). Спектр блочно-диагональной матрицы C является объединением СЗ блоков,

т.е. объединение блоков $\overline{Madj}$ и $ATAK$ не повлияют на значения СЗ матрицы $\overline{Madj}$, в которых находится секретная информация.

Шаг 3. Моделирование атаки. Проведение атаки осуществляется появлением ребер между вершинами-листьями графа СК и графа противника. Вес ребер моделирует силу атаки. В результате блочно-диагональная структура матрицы C будет разрушена появлением связей между элементами блока $ATAK$ и блока $\overline{Madj}$. СЗ матрицы $\overline{Madj}$ получат возмущения. Итогом атаки является матрица $\overline{C}$.

Шаг 4. Анализ спектра $\overline{C}$. Построить нормальное спектральное разложение матрицы $\overline{C}$.

а) если возмущения, которые произошли в ходе моделирования атаки, не затронули те СЗ, в первоначальных возмущениях которых хранится секретная информация, или лишь незначительно возмутили их (результат возмущающего воздействия сравним с шумом округлений), то СК устойчив к предполагаемой атаке. Устойчив также и СА его сформировавший;

б) если условие а) не выполнено то ставится задача выбора СА путем сравнения устойчивости имеющихся в наличии стегоалгоритмов $СА_1$, …, $СА_n$ к предполагаемой атаке. Для каждого из сформированных стеганоконтейнеров $СК_1$, …, $СК_n$ следует построить нормальное спектральное разложение их матриц $\overline{C}_1$, …, $\overline{C}_n$ и вычислить усредненные относительные погрешности $\delta_{1(cp)}$, …, $\delta_{n(cp)}$. Наименьшая из $\delta_{i(cp)}$ соответствует алгоритму, который следует выбрать для формирования СК.

3. Практическая реализация предложенного метода

В [6] представлен стегоалгоритм Stego_Graph, разработанный для идеального канала связи и обеспечивающий 100% правильно декодируемой информации. Погружение СИ происходит в пространственную область контейнера – изображения, которое предварительно разбивается на блоки, путем корректировки яркости пикселей. Каждый блок содержит восемь информационных элементов. Весовой коэффициент защиты ИЭ определяется как разность между исходным значением яркости и полученным после стегопреобразования.

Пример взвешенного графа-модели СК для одного блока, иллюстрирующий возможное соотношение между весовыми коэффициентами вершин разных уровней, представлен на рис. 2 (рядом с узлом – его номер, внутри узла – его вес).

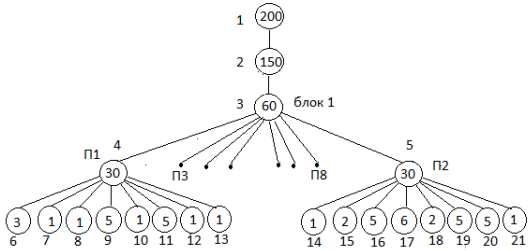

Рисунок 2 – Пример взвешенного графа-модели СК, построенного для одного блока

Матрица смежности $\overline{G}$ для ветви взвешенного графа, соответствующей подмножеству информационных элементов П1 (Рис. 2) имеет вид:

$$\overline{G} = \begin{bmatrix} 200 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 150 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 60 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 30 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 5 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Возмущающие воздействия на СК естественно моделировать при помощи наложения на его матрицу различных шумов. Часто используемой моделью для ошибок квантования, возмущающих воздействий в канале связи и атак на СК является аддитивный гауссовский шум [5].

Атаку будем моделировать в виде аддитивного гауссовского шума с нулевым средним и дисперсией равной 20 (в компьютерной системе MatLab, в которой проводился вычислительный эксперимент нормированное значение дисперсии такого шума равно 0.0003). Такой уровень шума еще не нарушает надежность восприятия СК, но каждый лист графа подвергается атаке. Один из возможных вариантов шума такого уровня в числовом представлении имеет вид: -3, 3, 3, 4, 1, -5, -3, 3, который накладывается на листья с номерами вершин 6 - 13 соответственно (Рис. 2).

Построим графово-матричную модель противника. Между членами последовательности, моделирующей шум, каждому из которых отвечает вершина графа-модели противника, отсутствует какая-либо связь, поэтому ребра между вершинами графа противника отсутствуют и такой граф представляет собой множество изолированных вершин. Поскольку

на СК накладывается шум одного уровня, то все вершины имеют одинаковый вес равный дисперсии, т.е. 20. Матрица такого графа будет диагональной, а ее диагональные элементы равны 20.

Построим совокупную графово - матричную модель СК и противника:

$$C = \begin{pmatrix} \overline{G} & 0 \\ 0 & ATAK \end{pmatrix}.$$

Спектр блочно-диагональной матрицы является объединением СЗ блоков. Спектр матрицы C для рассматриваемого примера состоит из следующих значений:

200.0200 150.0216 60.0485 30.1456 20.0000 20.0000 20.0000 20.0000 20.0000 20.0000 20.0000 20.0000 **5.0005 5.0000 3.0002 1.0010 1.0000 1.0000 1.0000 1.0000**

Жирным шрифтом выделены СЗ, которые соответствуют вершинам-листьям, т.е. пикселям, которые осуществляют защиту ИЭ.

Атаку осуществляем вводом новых ребер между вершинами графа противника и листьями графа СК, что приведет к появлению новой связи между диагональными элементами блока $ATAK$ и элементами блока $\overline{G}$. Вес ребер определяется гауссовским шумом с параметрами, описанными выше. Итогом атаки является матрица $\overline{C}$ (Рис. 3). СЗ матрицы $\overline{C}$ выглядят следующим образом:

200.0200 150.0216 60.0485 30.1456 21.5110 20.9980 20.5130 20.4624 20.4624 20.4624 20.4593 20.0524 **3.9812 3.4668 2.4662 0.9302 0.5376 0.5376 0.5376 0.4535**

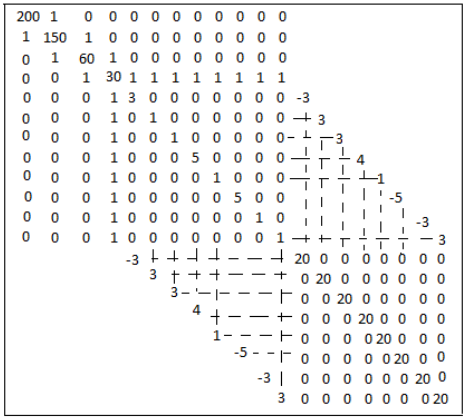

Рисунок 3 – Матричная модель атакованного СК

Как не трудно заметить, СЗ претерпели достаточные возмущения. Относительная погрешность δ для СЗ, выделенных жирным шрифтом: 0.2560 0.4423 0.2165 0.0761 0.8601 0.8601 0.8601 1.2051. Усредненная погрешность: $\delta_{1(cp)} = 0{,}5970$.

Для рассматриваемого примера атака, разрушающая защиту всех листьев, выражается реберными весовыми коэффициентами: 3 1 1 5 1 5 1 1 (знак коэффициента не имеет значения, поскольку на возмущение СЗ влияет абсолютная величина коэффициента (Лемма Гершгорина [7] о локализации СЗ)).

Рассмотрим другое подмножество пикселей, с весовыми коэффициентами их защищенности: 1, 2, 5, 6, 2, 5, 5, 1, представляющее подмножество П2. Предпримем ту же атаку. Для построения матричной модели не атакованного и атакованного СК выполним действия, изложенные выше.

Спектр матрицы C:

200.0200 150.0216 60.0495 30.1513 20.0000 20.0000 20.0000 20.0000 20.0000 20.0000 20.0000 20.0000 **5.9792 5.0000 5.0000 4.9338 2.0000 1.9591 1.0000 0.9567**

Спектр матрицы $\overline{C}$:

200.0200 150.0216 60.0497 30.1526 21.5110 21.0600 20.5777 20.5754 20.4860 20.4624 20.4608 20.0553 **4.9193 4.4223 4.3805 3.4661 1.9247 1.4924 0.5376 0.4959**

δ: 0.2155 0.1306 0.1414 0.4234 0.0391 0.3127 0.8601 0.9292

$\delta_{2(cp)} = 0{,}3815$

Сравнивая $\delta_{1(cp)}$ и $\delta_{2(cp)}$ можно сделать вывод что подмножество пикселей П2 более предпочтительно для погружения СИ.

Поскольку Stego_Graph для каждого блока формирует стегопуть по одному и тому же алгоритму, то мы не можем в одном и том же блоке выбирать наилучшие восемь пикселей в смысле их весовых коэффициентов. Поэтому для повышения устойчивости Stego_Graph было предложено выбрать наиболее подходящие блоки для встраивания СИ, основываясь на значениях их усредненной относительной погрешности. В результате такого подхода была повышена эффективность декодирования СИ в условиях присутствия шума на 15%.

Рассмотрим другой стегоалгоритм Stego_Graph1 [8]. Этот алгоритм для всех ИЭ обеспечивает весовой коэффициент равный семи. Для Stego_Graph1 получены следующие результаты:

Спектр матрицы C:

200.0200 150.0200 60.04151 30.1653 20.0000 20.0000 20.0000 20.0000 20.0000 20.0000 20.0000 20.0000 7**.000** 7**.000** 7**.000** 7**.000** 7**.000** 7**.000** 7**.000** **6.8147**

Спектр матрицы $\overline{C}$:

200.0200 150.0200 60.04151 30.1668 21.6971 21.1297 20.6589 20.6589 20.6589 20.6589 20.6511 20.0763 **6.9048 6.3411 6.3411 6.3411 6.3411 6.2368 5.8416 5.2758**

δ: 0.0138 0.1039 0.1039 0.1039 0.1039 0.1224 0.1983 0.2917

$\delta_{3(ср)} = 0{,}1302$

В этом случае все ИЭ защищены в полной мере – СЗ после атаки изменились незначительно, более того, Stego_Graph1 обеспечит защиту и при увеличении значений атаки до ± 7 на каждый информационный элемент.

Выводы

Таким образом, получил дальнейшее развитие общий подход к анализу состояния и технологии функционирования информационных систем, что дало возможность провести анализ некоторых СА в рамках построенной графовой модели СК, а также повысить устойчивость СА путем их модификации. Так устойчивость новой модификации базового стегоалгоритма Stego_Graph повышена на 15% за счет анализа и выбора блоков для погружения СИ, что является доказательством адекватности построенной модели СК. Предложено методику сравнения параметров, а именно СЗ, матриц контейнера и СК, созданных различными СА, которая позволила получить априорную оценку устойчивости СА и выбрать из множества алгоритмов наиболее устойчивый.

Список использованных источников: **1.** *Ленков С.В. Методы и средства защиты информации: в 2 т. / С.В.Ленков, Д.А.Перегудов, В.А. Хорошко. – К.: Арий, 2008. – 464 . – Т.2: Информационная безопасность. – 2008. – 344 с.* **2.** *Харари Ф.* Теория графов / *Ф.Харари*; пер.с англ. *В.П.Козырева*. – М.: Мир, 1973. – 300 с. **3.** *Кобозева А.А. Анализ информационной безопасности / А.А.Кобозева, В.А. Хорошко. – К.: Изд. ГУИКТ, 2009. – 251 с.* **4.** *Кобозева А.А. Загальний підхід до оцінки властивостей стеганографічного алгоритму, заснованій на теорії збурень / А.А. Кобозева// Информационные технологии и компьютерная инженерия. – 2008. – №1(11). – С.164-171.* **5**. *Gkizeli M. Optimal Signature Design for Spread-Spectrum Steganography / M.Gkizeli, D.A.Pados, M.J.Medley // IEEE Trans. On Image Processing. – 2007. – Vol.16, № 2. – P. 1021-1031.* **6.** *Борисенко И.И. Особенности применения многоуровневого порогового преобразования изображения в компьютерной стеганографии / И.И. Борисенко // Праці УНДІРТ. – 2006. – №4(48). – С. 53 – 59.* **7.** *Гантмахер Ф.Р. Теория матриц / Ф.Р. Гантмахер. – М.:Наука, 1988. – 552с.* **8**. *Борисенко И.И. Повышение помехоустойчивости стеганографического алгоритма / И.И.Борисенко// Сучасний захист інформації. – 2010. – №1. – С. 36-42.*

Bibliography (transliterted): **1.** *Lenkov S.V.* Metody i sredstva zashhity informacii: v 2 t. / *S.V.Lenkov, D.A.Peregudov, V.A. Horoshko*. – K.: Arij, 2008. – 464 . – T.2: Informacionnaja bezopasnost'. – 2008. – 344 s. **2.** *Harari F.* Teorija grafov / *F.Harari*; per.s angl. *V.P.Kozyreva*. – M.: Mir, 1973. – 300 s. **3.** *Kobozeva A.A.* Analiz informacionnoj bezopasnosti / *A.A.Kobozeva, V.A. Horoshko*. – K.*:* Izd. GUIKT, 2009. – 251 s. **4.** *Kobozeva A.A.* Zagal'nij pidhid do ocinki vlastivostej steganografichnogo algoritmu, zasnovanij na teorii zburen' / *A.A. Kobozeva* // Informacionnye tehnologii i komp'juternaja inzhenerija. – 2008. – №1(11). – S.164-171. **5.** *Gkizeli M.* Optimal Signature Design for Spread-Spectrum Steganography / *M.Gkizeli, D.A.Pados, M.J.Medley* // IEEE Trans. On Image Processing. – 2007. – Vol.16, № 2. – R. 1021-1031. **6**. *Borisenko I.I.* Osobennosti primenenija mnogourovnevogo porogovogo preobrazovanija izobrazhenija v komp'juternoj steganografii/ I.I. *Borisenko* // Praci UNDIRT. – 2006. – №4(48). – S. 53-59. **7**. *Gantmaher F.R.* Teorija matric / F.R. Gantmaher. – M.:Nauka, 1988. – 552 s. **8**. *Borisenko I.I.* Povyshenie pomehoustojchivosti steganograficheskogo algoritma / I.I.Borisenko // Suchasnij zahist informacii. – 2010. – №1. – S. 36-42.